REMARKS

The claims have been amended to more clearly define the invention as disclosed in the written description. In particular, claim 9 has been made a proper independent claim. In addition, the claims have been amended for clarity.

Applicant believes that the above changes answer the Examiner's objections to the claims, and respectfully requests withdrawal thereof.

The Examiner has rejected claim 10 under 35 U.S.C. 101 in that the claim, directed to functional descriptive material, is non-statutory. Applicant has amended claim 10 to claim a computer-readable medium having the computer program product recorded thereon. As such, Applicant believes that claim 10 is now statutory.

The Examiner has rejected claims 1-3 and 7 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,209,092 to Linnartz in view of U.S. Patent 6,888,944 to Lotspiech et al. The Examiner has further rejected claims 4-6 and 8-10 under 35 U.S.C. 103(a) as being unpatentable over Linnartz in view of Lotspiech et al. with "incorporated by reference" of U.S. Patent 6,118,873 to Lotspiech et al.

The Linnartz patent discloses a method and system for transferring content information and supplemental information relating thereto, in which two separate conditions need to be verified for a storage medium before playback is allowed, i.e., verification of a watermark embedded in the data recorded on the

storage medium, and verification of a modulation pattern of variations of a physical parameter representing a medium mark P.

The Lotspiech et al. '944 patent discloses a method for assigning encryption keys for, for example, to enable authorized player-recorders to play and/or copy encrypted music videos and other content. To that end, "A method is disclosed for defining sets of encryption keys from a key matrix. The method includes receiving parameters representing characteristics (such as the number of rows and columns) of the key matrix, and, using the parameters and an error-correcting code such as but not limited to a linear code, defining plural sets of keys. The sets of keys are then assigned to respective player-recorder devices. By "error-correcting code" is meant a non-random function that generates plural sets of keys with a prescribed Hamming distance between every two sets of keys." (col. 2, lines 24-33).

The subject invention relates to the reliable recovery of cryptographic data obtained from a property of a storage medium, which tolerates small deviations in the measured value of the property of the storage medium. To that end, the subject invention includes "obtaining cryptographic data from a property of the storage medium", "reading helper data from the storage medium" and "granting the access based on an application of a delta-contracting function to the cryptographic data and the helper data".

The Examiner has indicated that Linnartz discloses "obtaining cryptographic data from a property of the storage medium" (i.e., the medium mark P), and recovering supplemental

information (i.e., watermark W) embedded with the content of the storage medium. The Examiner now considers this supplemental information as "helper data" as claimed in, for example, claim 1. The Examiner then notes "Linnartz does not disclose expressly "granting the access based on an application of a delta-contracting function to the cryptographic data (Y) and the helper data (W)".

Applicant submits that there is an error in the Examiner's analysis. In particular, there is no disclosure or suggestion in Linnartz that the cryptographic data and the supplemental information should in some way be combined. In fact, Linnartz specifically states, at col. 8, lines 60-67, "The medium mark allows two separate conditions to be verified for an original disc before playback is allowed", i.e., verification of the watermark and verification of the medium mark P. However, there is no disclosure that these two should somehow be combined.

The Examiner then uses Lotspiech et al. '944 patent to show the application of a delta-contracting function in generating decryption keys, and states "Lotspiech teaches an effective mechanism to store / retrieve the cryptographic security keys with a compact data storage structure of crucial key elements for an authorized player-recorder apparatus".

Applicant submits that the Examiner is mistaken. In particular, Lotspiech et al. does not teach an effective mechanism to store/retrieve the cryptographic security keys, but rather a way of generating decryption keys that are then stored in the various player/recorder devices.

Applicant further submits that the only relation between Linnartz and Lotspiech et al. is that they are concerned with the encryption/decryption of data. However, since there is no disclosure or suggestion of combining the two recovered data in Linnartz, then there is no suggestion to apply these two recovered data in the delta-contracting function disclosed in Lotspiech et al. '944 patent for use in generating decryption keys for storing in player/recorder devices.

The Lotspiech et al. '873 patent discloses a system for encrypting broadcast programs in the presence of compromised receiver devices. However, Applicant submits that Lotspiech et al. '873 patent does not supply that which is missing from Linnartz and Lotspiech et al '944 patent.

In view of the above, Applicant believes that the subject invention, as claimed, is not rendered obvious by the prior art, and as such, is patentable thereover.

Applicant believes that this application, containing claims 1-10, is now in condition for allowance and such action is respectfully requested.

Respectfully submitted,

by /Edward W. Goodman/
Edward W. Goodman, Reg. 28,613
Attorney
Tel.: 914-333-9611